OGC 79-00135
4 January 1979

MEMORANDUM FOR : General Counsel

25X1 FROM : [redacted]

SUBJECT : Collection of Foreign Intelligence Concerning U.S. Persons - Comparison of S.2525 With, and Effect Upon, Present Practices and Procedures

OVERVIEW of CURRENT PRACTICE

1. You have requested an overview, in connection with the deliberations of the Administration's Intelligence Charter Legislation Task Force chaired by David Aaron, of present authorities, practices and procedures regarding the collection of foreign intelligence information concerning U.S. persons, the relevant provisions of S.2525, and the impact of S.2525 if enacted into law. As you suggested, I have treated electronic surveillance and physical searches separately and have subsumed all other techniques in the discussion of general collection authorities.

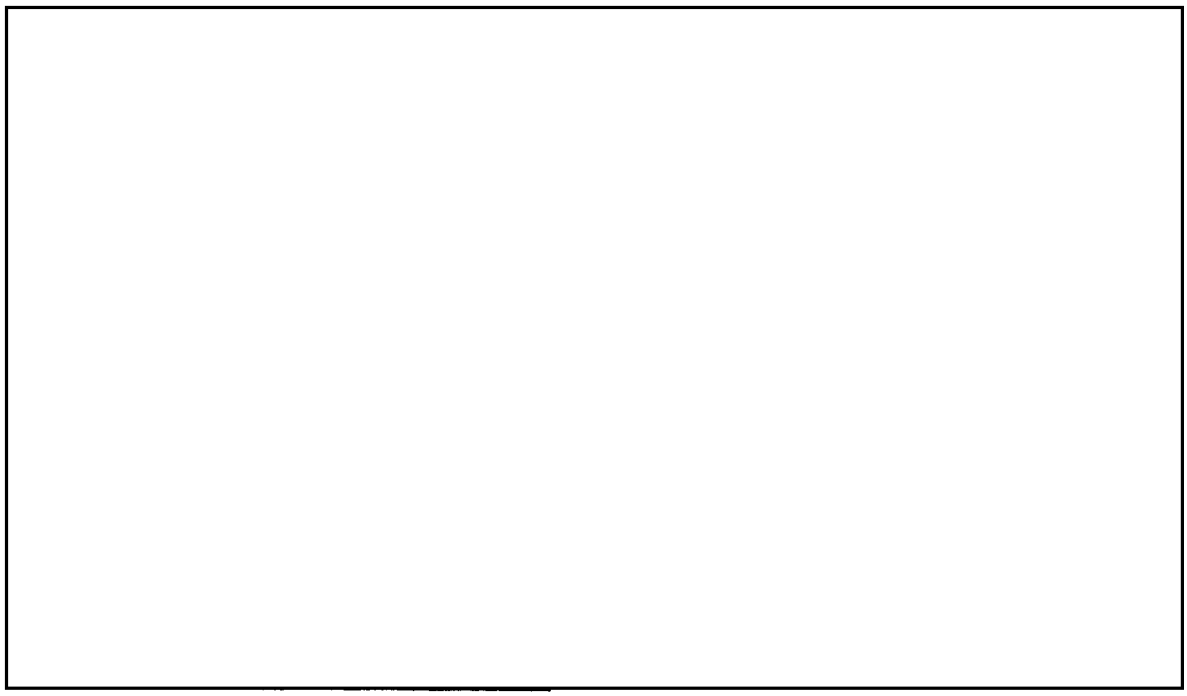
I. Electronic Surveillance

25X1

2. Within the United States:

[redacted]

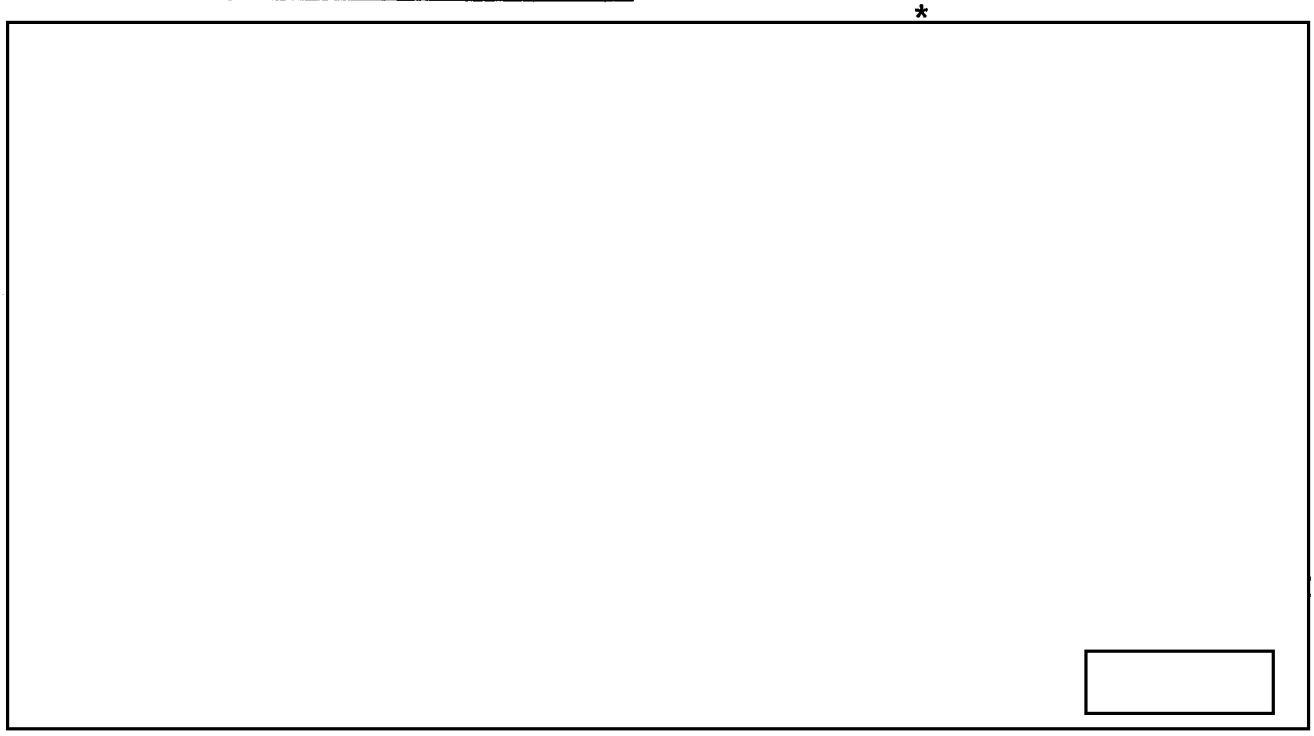
25X1



25X1

25X1

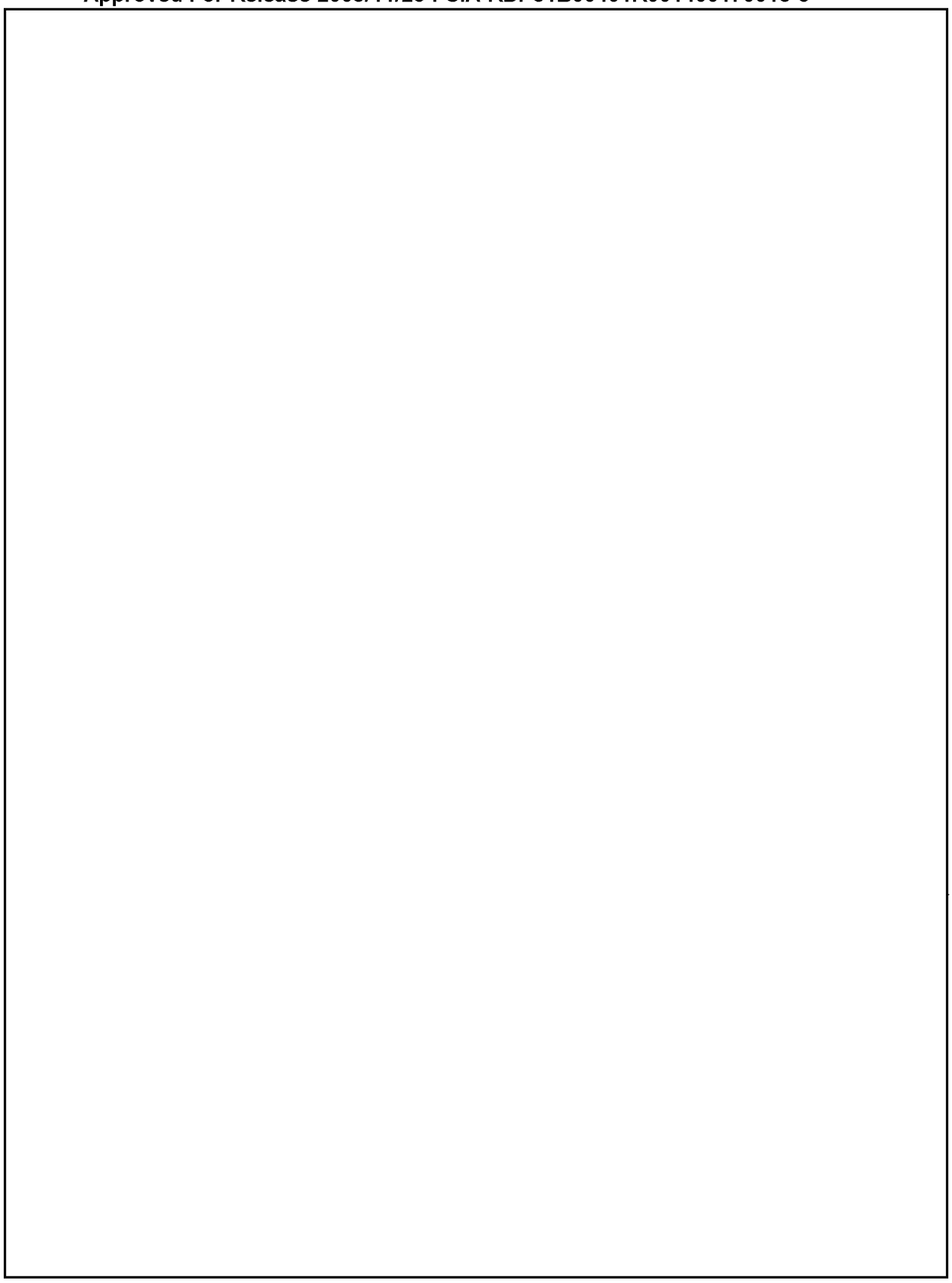
3. Outside the United States:*



5X1

*It should be noted throughout this paper that the procedures referred to are those developed under E.O. 11905 which have been continued in force by E.O. 12036 until the ongoing process of developing new procedures under E.O. 12036 is completed.

25X1



Next 3 Page(s) In Document Exempt

Approved For Release 2005/11/23 : CIA-RDP81B00401R001400170018-3

clandestine intelligence activities for or employed by foreign powers or are fugitives from U.S. justice with significant relations with foreign governments.

25X1

cc: Hoskinson/NSC Staff
25X1 OLC/
25X1 C/
25X1 DCI/

25X1 OGC/

Distribution:
Orig-Addressee & File OGC Subj LEGISLATION (ARC holding) n.i.
1-AAL Signer
1-ARC Signer
1-OGC Chrono

1/5/79

SSCI Position Paper

TITLE II SUMMARY

I. General Principles

The following principles would be established at the beginning of title II--

SSCI POSITION PAPER

A. All activities undertaken by entities of the intelligence community shall be designed and conducted so as not to limit, disrupt, or interfere with the full exercise of rights protected by the Constitution and laws of the United States.

B. No entity of the intelligence community may collect private information concerning any unconsenting U.S. person solely on the basis of the religious or political views expressed by that person or that person's exercise of any right protected by the Constitution or laws of the United States.

C. No information acquired by any entity of the intelligence community may be used or disclosed by Federal officers or employees except for lawful purposes.

D. No person, when acting on behalf of an entity of the intelligence community may-- (a) participate in unlawful acts of violence; (b) use unlawful means to obtain information; (c) initiate a plan to commit unlawful acts; or (d) participate in any other unlawful activity, except insofar as the entity head or a designee determines under procedures approved by the Attorney General that such participation is necessary for lawful purposes.

II. Procedural Requirements

A. Approval of Procedures

All collection of private (i.e., non-publicly available) information from or concerning U.S. persons, or other persons within the United States, without their consent would be governed by procedures approved by the Attorney General, except that--

(a) procedures for collection directed against members of the Armed Forces would be approved jointly by the Secretary of Defense and the Attorney General;

(b) procedures for collection directed against entity employees would be approved jointly by the entity head and the Attorney General.

The Attorney General would evaluate the procedures regularly to determine whether they adequately meet the requirements of this title, and make such recommendations for changes therein as may be necessary to meet those requirements.

B. Basic Requirements

The procedures would-- (a) ensure that the least intrusive means are used that will acquire information of the nature, reliability, and timeliness that is required; (b) designate officials who may approve collection and the use of particular techniques; and (c) include any other requirements needed to protect constitutional rights and privacy and limit the use of information to lawful governmental purposes.

C. Reporting of Procedures

The procedures and any changes thereto would be reported to the Intelligence Committees at least sixty days prior to their effective date, unless the Attorney General determines immediate action is required and notifies the committees immediately of such procedures and the reason for their becoming effective immediately.

D. Duration and Review

Initiation of collection of private information from or concerning any unconsenting U.S. person would require written approval by a designated official, valid for not more than six months and based on a finding that such collection is permitted under this title. Collection that continues beyond six months would require written approval every six months by the entity head or a designee, based on a finding that specific facts and circumstances justify continuation. Collection that continues beyond a year would be reviewed annually by the Attorney General or a designee (except for entity employees and members of the Armed Forces).

III. Standards for Collection

A. Counterintelligence and Counterterrorism Intelligence

1. Basic standards. There would be separate standards for collection against U.S. persons in the United States and abroad. A criminal standard would be required in the United States unless the person knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power and contrary to the interests of the United States. There would be a non-criminal standard abroad covering any person who knowingly acts outside the United States for or on behalf of an intelligence or security service of a foreign power. The international terrorism standard would cover activities for or on behalf of foreign-based groups. (Domestic-based groups engaged in international terrorism would be included in the FBI law enforcement charter.)

2. Recruitment subjects. Collection would be limited to subjects of recruitment efforts to engage in activities that meet the basic standards (above). Mail covers, confidential records, and continuing covert participation in U.S. organizations could not be used under this standard.

3. Targets. Collection would be limited to targets of clandestine intelligence gathering activities, international terrorism, or foreign assassination attempts. Consent would be required unless a designated official determines that (a) obtaining consent would jeopardize specific

classified sources or methods, or (b) there is a reasonable possibility that the person may be cooperating in clandestine intelligence gathering or international terrorism. Mail covers, access to confidential records, and continuing covert participation in U.S. organizations could not be used under this standard.

B. Potential Sources

Consent would be required unless a designated official determines that obtaining consent would jeopardize specific classified sources or methods or the security of a specific intelligence activity. Mail covers, access to confidential records, and continuing covert participation in U.S. organizations could not be used under this standard.

C. Foreign Intelligence

1. Prohibition. An entity may collect foreign intelligence from or concerning any U.S. person only--(a) with that person's consent; (b) from publicly available sources or persons who volunteer such information; (c) if the information does not identify the person and is not collected from that person, directly or indirectly; (d) if the person is the subject of collection under the basic counterintelligence and counterterrorism intelligence standards; or (e) under a Presidential waiver (see below).

2. Presidential waiver. The President may authorize the Attorney General to approve specific procedures for such collection if the President makes a written determination that-- (a) the proposed collection is necessary and proper to obtain information concerning foreign powers, organizations, or persons that is in the possession or or requires identification of U.S. persons; (b) the type of information to be collected is vital to the conduct of the foreign relations or the protection of the national security of the United States; and (c) other means are not available to acquire information of the nature, reliability, and timeliness that is required.

3. Limits on the waiver. An entity may collect such intelligence under a Presidential waiver only--

(a) outside the United States, if the Director of National Intelligence approves such collection based on a written finding that specific facts and circumstances indicate that information in the possession of or requiring the identification of the person is the type authorized to be collected;

(b) if the entity head or a designee approves such collection based on a written finding that the subject is an entity directed and controlled by a foreign power; or

(c) if the information is obtained from cooperating sources to whom it has been disclosed previously and voluntarily.

No entity may collect such intelligence within the United States unless expressly authorized by statute to do so.

4. Procedures under the waiver. The procedures approved by the Attorney General must be reasonably designed to minimize the acquisition, retention, and dissemination of information that concerns religious or political views expressed by U.S. persons or their exercise of rights protected by the Constitution and laws of the United States. Other information identifying a U.S. person may be retained and disseminated only if it is the type authorized to be collected and that person's identity is necessary to understand such information or assess its importance.

5. Reporting. The Presidential waiver and the procedures approved thereunder would be reported in advance to the Intelligence Committees. On a quarterly basis the Director of National Intelligence would fully inform the committees concerning any collection approved by him under the waiver.

D. Security Investigations

1. Employees. There would be broad authority to collect information concerning entity employees, contractors, and employees of contractors knowingly employed on the contract with the entity.

2. Former employees. Former employees could be investigated abroad if facts and circumstances indicate that the person has violated or intends to violate any law or contractual obligation relating to the protection of classified intelligence sources or methods. Investigations within the United States would be conducted by the FBI and would require facts and circumstances indicating that the person has violated or intends to violate a federal statute relating to such protection, including a new criminal statute on unauthorized disclosure of sources.

3. Physical security threats. Information could be collected concerning any person engaged in activities that pose a direct and immediate threat to the physical safety of entity personnel or property. However, such activities in the United States must indicate a violation of federal, state, or local law, and collection must be limited to that necessary to refer the matter to an appropriate law enforcement agency. Mail covers, access to confidential records, and continuing covert participation in U.S. organizations could not be used in the United States under this standard.

4. Proximity inquiries. Collection would be limited to persons whose proximity to an intelligence activity may threaten its security. Mail covers, access to confidential records, and continuing covert participation in U.S. organizations could not be used under this standard.

E. Collection Concerning Non-U.S. Persons in the United States

The standards would authorize collection from or concerning foreign powers and any non-U.S. person--(a) who acts in the United States as an officer or employee of a foreign power, or as a member of an international terrorist group; (b) when the circumstances of the person's presence in the United States indicate that he may engage in clandestine intelligence activities; (c) when the entity head or a designee determines that the information sought from the person is significant foreign intelligence; or (d) when collection would be permitted if the person were a U.S. person.

Procedures for collection would be approved by the Attorney General in consultation with the appropriate entities, the Secretary of State, and the Director of National Intelligence and would-- (a) specify any necessary and proper departures from the limitations on duration and techniques applicable to U.S. persons, and (b) minimize incidental acquisition of information concerning U.S. persons and any inhibiting effects on the free exchange of ideas and information between U.S. persons and other persons within the United States.

IV, Retention and Dissemination of Private Information Concerning U.S. Persons

A. Alternatives

An alternative to the broad and detailed standards of S. 2525 should be considered.

1. S. 2525 Approach. That approach would spell out particular standards for retention, including any information that might reasonably provide the basis for initiating collection. Equally specific standards would be established for dissemination of foreign intelligence, counterintelligence and counterterrorism intelligence, as well as information relating to criminal activity, trustworthiness of persons having access to classified information, and suitability of potential sources.

2. Alternative Approach. An alternative would require minimization procedures approved by the Attorney General that--

(a) are reasonably designed in light of the circumstances in which the information was acquired to minimize retention and dissemination consistent with the functions and responsibilities of each entity authorized by this Act;

(b) allow dissemination of foreign intelligence in a manner that identifies a U.S. person only if that identity is necessary to understand or assess the information that is disseminated;

(c) allow retention and dissemination of criminal evidence for law enforcement purposes;

(d) allow dissemination to a Government employee if relevant to his lawfully authorized governmental functions;

(e) specify the circumstances in which particular types of information may be disseminated outside any entity that acquires the information; and

(f) allow dissemination to a foreign government only if the information is counterintelligence, counterterrorism intelligence, or criminal evidence of direct interest to that government and such dissemination is in the interests of the United States.

B. Unlawfully Acquired Information

Such information would be destroyed unless the entity head or a designee determines that the information-- (a) should be retained for oversight, accountability, or redress; or (b) relates to legal proceedings of which the entity has notice or reasonably may anticipate. Such information may also be retained and disseminated if the Attorney General determines that it indicates a threat of death or serious bodily harm to any person.

V. Collection Techniques

A. Intrusive Techniques

1. Approval. The entity head or a designee would approve collection using any or all of the following techniques against a U.S. person based on a written finding that specific facts and circumstances justify such collection--

(a) mail covers, if in accordance with Postal Service regulations;

(b) covert human sources (except pretext interviews by entity employees);

(c) access to confidential records when such access for law enforcement purposes is limited by law, if in accordance with applicable law.

The Attorney General or a designee would be notified promptly and could terminate such collection at any time (except for collection against entity employees and members of the Armed Forces).

2. Participation in U.S. organizations. When a covert human source is to participate in a U.S. organization to collect private information on a continuing basis concerning the organization, its members, or its employees, the entity head or a designee would make a separate written finding that--

(a) such participation is necessary and proper for collection under this title;

(b) the procedures for such participation are reasonably designed to minimize any influence on lawful

activities and any acquisition, retention and dissemination of information that concerns religious or political views expressed by U.S. persons or their exercise of rights protected by the Constitution and laws of the United States.

3. Unresolved Issues. The following principal issues should be considered--

(a) whether defined exceptions to U.S. laws relating to the confidentiality of certain records (e.g. tax, credit, or educational records) should be made to give entities of the intelligence community access to non-U.S. persons' records when necessary;

(b) whether it is intended that Postal Service regulations be modified for mail covers against either U.S. persons or non-U.S. persons;

(c) the form additional safeguards should take for undisclosed participation in U.S. organizations when the purpose is not to collect private information concerning the organization, its members, or its employees.

B. Searches within the United States

S. 1566 would apply, with warrantless searches limited to property under the open and exclusive control of an "official foreign power" if there is no breaking and entering of real property. The Attorney General's findings and procedures for warrantless searches would be reported to the Intelligence Committees at least thirty days in advance. A separate court order would be required for each physical search involving unconsented entry. The court would determine whether the facts justify opening more than one article of mail or conducting more than one physical search that does not involve unconsented entry.

C. Electronic Surveillance and Searches Targeted Against U.S. Persons Abroad

1. Court order procedures. The court order procedures in S. 1566 would apply in virtually all respects, but with a restriction against disclosing liaison relationships to the court. An exception to the court order requirement might be permitted if the Attorney General determines that information needed to obtain a court order cannot be disclosed to the court because of objections by a foreign government that provided the information and that all practicable efforts have been made to obtain permission to disclose the information. The Intelligence Committees would be fully informed within ten days concerning any such exception.

2. Targeting standards. Targeting would be permitted when the U.S. person (a) would meet the S. 1566 criminal standard if his activities were conducted in the United States; (b) is an entity directed and controlled by a foreign power; (c) resides abroad and acts as an officer or employee of a foreign power; or (d) is a fugitive from U.S. justice abroad whose relationship with a foreign power is likely to constitute foreign intelligence. Targeting might also be permitted if a U.S. person knowingly acts outside the United States pursuant to the direction of a foreign power and such person's communications or activities are likely to constitute foreign intelligence (as defined in S. 1566).

3. Relationship to S. 1566. Nothing in this Act could be construed to modify S. 1566. The provisions of S. 1566 regarding administration, security, appeals, use of information, and reporting would apply to electronic surveillance and searches under this title.

D. Minimization Procedures for Untargeted Surveillance

Minimization procedures comparable to S. 1566 and approved by the Attorney General would apply to electronic surveillance abroad and would be reported to the Intelligence Committees at least sixty days in advance. A separate restriction for communications known to be between U.S. persons would permit retention and dissemination if the contents are

not disseminated in a manner that identifies either party, with an exception allowing such dissemination of an identity if the Attorney General determines that it indicates a threat of death or serious bodily harm to any person.

VI. Other Provisions

1. Title II Provisions

The following provisions from title II of S. 2525 would be substantially retained in title II-- (a) assistance to law enforcement authorities; (b) human experimentation; (c) criminal sanctions; (d) civil damages; (e) administrative sanctions; (f) protection of privileged communications; and (g) administrative rulemaking.

1. Title I Provisions

The following provisions from title I of S. 2525 would be substantially retained in title I-- (a) restrictions on the use of certain categories of individuals for certain intelligence activities; (b) requirements for sensitive intelligence collection projects and special activities; (c) requirements for counterintelligence and counterterrorism activities; (d) Presidential waiver of the application of certain restrictions and prohibitions in time of war; (e) prohibitions and restrictions on activities undertaken indirectly; and (f) restrictions on contracting.